Patent claims

1. A method for operating a security module, having the following features:

- the security module comprises a secure key memory and at least one data interface.
- in a personalization state a connection to a personalization unit is set up using the data interface.
- the security module is used to create a module key pair afresh and to store it in the key memory.
- the public module key is sent to the personalization unit via the connection.
- the personalization unit produces a certificate about the public module key by signing with a signing key from the personalization unit, sends it to the security module and stores it securely therein.
- the connection is then cleared down; the security module changes from the personalization state to the operating state.
- in the operating state a cryptographically secure connection to a central system is set up, said connection involving the use of the private module key and involving the public module key together with the certificate being transmitted to the central system, where the certificate is checked.

2. The method as claimed in claim 1, where fresh changeover to the personalization state erases the module key.

3. The method as claimed in claims 1 or 2, where in the personalization state the connection between the security module and the personalization unit is checked cryptographically

for authenticity and is protected against corruption.

4. The method as claimed in one of claims 1 to 3, where a public key from the central system is transmitted together with the module certificate, said key being used in the operating state to check the authenticity of the central system.

5. The method as claimed in claim 4, where the public key from the central system is signed with the signing key from the personalization unit, and the resultant certificate is transmitted too and is checked by the security module.

6. The method as claimed in claim 5, where the signer's public signing key is signed by the central system, and this certificate is transmitted too and is checked by the security module.

7. The method as claimed in one of claims 1 to 6, where

- the key memory in the security module stores a public checking key from the manufacturer,
- the personalization unit transmits its public signing key together with a certificate, formed with the checking key from the manufacturer,
- and the security module first checks the public signing key's certificate with the public checking key and then checks the certificates produced with the public signing key,
- and changes to the operating state only if the check is successful.

8. The method as claimed in one of claims 1 to 7, where the security module is used to form a permanent

identity key on a one-off basis, the associated public key is signed with the checking key from the manufacturer, and the corresponding certificate is stored in the security module. The identity key with a certificate is used to assure the personalization unit of authenticity on the basis of a challenge-response method.

9. The method as claimed in one of claims 1 to 8, where the security module sends the personalization module a time stamp or random value which is included in the signature too when the certificates are formed.

10. The method as claimed in one of claims 1 to 9, where the personalization system sends a variation value to the security module, which is used when the new module key is produced.

11. The method as claimed in one of claims 1 to 10, where the connection to the central system which has been set up using the private module key is used to interchange a symmetrical key for subsequent transaction connections and to store it in the secure key memory in the security module.

12. The method as claimed in one of claims 1 to 11, where a mobile personalization unit is used which is connected to the security module directly via a connection which is controlled by a user.

13. The method as claimed in one of claims 1 to 12, where a user inputs a one-off transaction number into the security module, either directly using an input unit which is connected permanently to the security module or immediately and directly using an input unit which is connected to the security module by the user, and the

connection to the personalization unit is protected by transmitting the transaction number.

14. The method as claimed in one of the previous claims, where a mobile appliance is connected to the personalization unit via a local connection to the security module, which local connection is controlled directly by a user, and a long-distance connection, the mobile appliance identifies itself to the personalization unit, and as a result the security module is indirectly identified to the personalization unit.

15. The method as claimed in claim 14, where the local and long-distance connections are used merely for securely setting up a secure direct network connection between the security module and the personalization unit.

16. A method for personalizing a security module, having the following features:

- the security module is connected to a personalization unit.
- the security module is connected temporarily to an identification unit by a user using an interface which is determined by the user.
- the identification unit sends an identification value, which can be checked by the personalization unit, to the security module, which forwards it to the personalization unit.
- the personalization unit performs the personalization if the check on the identity value is positive.

17. The method as claimed in claim 16, where the identification value is a one-off transaction number produced beforehand.

18. The method as claimed in claim 17, where the identification value is interchanged between

the identification unit and the personalization unit using a cryptographically authenticated data connection.

19. A security module, containing a secure key memory, a programmable processor and at least one data interface, where the programming of the processor causes the security module to behave in line with one of claims 1 to 15.

20. A personalization unit, containing a secure key memory, a programmable processor and at least one data interface, where the programming of the processor causes the personalization unit to behave in line with one of claims 1 to 15.

21. A central system, containing a secure key memory and at least one data interface, where the programming of the central system causes the central system to behave in line with one of claims 1 to 15.